REMARKS

This amendment is submitted in response to the Office Action of December 17, 2004. Reconsideration and allowance of the claims is requested.

In this Office Action, claims 5-8 and 10-17 are examined. Claim 5 and the claims dependent on it are rejected under 35 U.S.C. § 112 as being unclear. Claims 5-6 and 12-17 are rejected as claiming unclaimed subject matter. Claims 5-8 and 10-17 are rejected over prior art. The above rejections are traversed and reconsideration and allowance of the claims is requested.

Claim 5 is rejected under 35 U.S.C. § 112 for using a limitation "the receiver's public key." Therefore, appropriate amendment to claim 5 has been made to eliminate this issue.

Claims 5-6 and 12-17 are rejected for claiming non-statutory subject matter. This rejection is respectfully traversed, as the claims as submitted clearly recite utilization of a PEAD to carry out the steps of the method. However, in an effort to move the prosecution forward, the Examiner's suggestions have been adopted.

Claims 5-8 and 10-11 are rejected under 35 U.S.C. § 102 (e) as anticipated by *Dorenbos*, U.S. 5,751,813. This rejection is respectfully traversed. In our claimed invention, the server does not perform any encryption or decryption and our server simply serves as a message relay server and public key directory server. On the contrary, *Dorenbos* teaches a unit 103 encrypts a message and send to the encryption server 101, the encryption server first need to decrypt the message (column 3 line 26-27) and then encrypt the message using the recipient public key (column 3 line 30-36) and send out the resultant re-encrypted message to recipient. Compared with our invention, our system is much more secure than the *Dorenbos* method. Because in our invention, the message was encrypted by the user (see lines 6-7, claim 5) and the server does not have a key to decrypt the message (remember the user public key cannot decrypt the message encrypted by a shared secret! *Dorenbos* column 3 lines 12-15 does not teach how to derive share secret at all. The first-stage encryption taught by *Dorenbos* is not a shared secret derivation, it is a simple server public key encryption which is a similar technique used in the popular SSL class-2 encryption in today's internet browser) and only the recipient has the key to decrypt the message as claimed.

The message remains encrypted even in the server. Therefore there is no man-in-the-middle attack can compromise the security. On the contrary, *Dorenbos* method reveals a single point of attack weakness in the server. If any hacker can access the server, then the entire system security will be compromised, because the server has the capability to decrypt any message goes through the server.

Therefore, in view of these clear distinctions, which are supported by the claim language, reconsideration and withdrawal of the rejection is requested.

Claim 12 is rejected under 35 U.S.C. § 103 as being unpatentable over *Dorenbos* in view of *Spies et al.*, U.S. 6,055,314. This rejection is respectfully traversed. Downloading key pairs taught in Spies column 6 lines 56 - column 7 lines 3) is a very un-secure method. It opens up a potential man-in-the-middle attack to intercept the user private key over the network and compromise the security of the whole system. Our invention insists that private key has to be generated by the user device such as PEAD. During the life time of the user private key, the user private key is never exposed to outside world nor ever been transmitted outside of the user device, therefore totally eliminating the security hole of *Spies*.

Claims 13-17 are rejected under 35 U.S.C. § 103(a) as unpatentable over *Dorenbos* taken with *Blakely*, U.S. 5,677,952. This rejection is respectfully traversed. These claims depend on either claims 5 or 6 whose patentability has been established above. Claims 13-17 are patentable for the same reasons discussed above with respect to claims 5-8, 10 and 11.

Security is a very delicate matter. A lot of methods look secure but simply are not secure after been attacked. It is not obvious to invent a secure system. By putting a private key and public key into a system does not automatically make it secure or teach anything secure! They must be properly used and stored. The claimed system provides a level of security for above that suggested by the references. Therefore, all of the above claims should be allowed.

In order to expedite the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney if any issues remain outstanding after receipt and consideration of this response.

Having addressed all issues set out in the office action, Applicant respectfully submits that the claims are in condition for allowance and respectfully request that the claims be allowed.

Respectfully submitted,

James A. Sheridan
Registration No. 25,435
MOSER, PATTERSON & SHERIDAN, L.L.P.
3040 Post Oak Blvd. Suite 1500
Houston, TX 77056
Telephone: (713) 623-4844
Facsimile: (713) 623-4846